

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

DIEGO FABIAN CAMARGO OCHOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
TUNJA
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

DIEGO FABIAN CAMARGO OCHOA

Diplomado de opción de grado presentado para
optar el título de INGENIERO DE SISTEMAS

DIRECTOR:
Ing. JAVIER RICARDO VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
TUNJA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del
Jurado

Firma del Jurado

Firma del Jurado

TUNJA, 29 de noviembre de 2021

AGRADECIMIENTOS

Después de una época académica de varios esfuerzos y aprendizajes, viendo ya alcanzado una nueva etapa de mi proyecto de vida, doy gracias a Dios por guiar cada paso para llegar hasta aquí, a mi familia por el apoyo incondicional que siempre me han brindado y a los profesores por el conocimiento que aportaron para mi vida profesional.

Es gratificante mirar atrás y recordar como inicio una etapa y como con enfoque y perseverancia se logró construir un sueño, porque no es fácil trabajar y estudiar a la vez, se convierte en todo un reto, pero somos lo que nos proponemos en la vida; y así, tengo la certeza que todo será posible.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN	10
DESARROLLO	11
1. Escenario 1	11
2. Escenario 2	24
CONCLUSIONES	54
BIBLIOGRAFÍA.....	55

LISTA DE TABLAS

Tabla 1. Direccionamiento Item. _____	2
Tabla 2. Tareas de configuración para R1 -----	12
Tabla 3. Tareas de configuración para S1 -----	16
Tabla 4. Configuración de equipos PC_A -----	19
Tabla 5. Configuración de equipos PC_B -----	20
Tabla 6. Inicialización de Dispositivos-----	29
Tabla 7. Configuración servidor internet-----	33
Tabla 8. Configuración Router R1-----	33
Tabla 9. Configuración Router R2-----	37
Tabla 10. Configuración Router R3-----	40
Tabla 11. Configuración Swith S1-----	42
Tabla 12. Configuración Swith S2-----	43
Tabla 13. Verificación de la red_____	44
Tabla 14. Configuración routing entre VLAN -----	45
Tabla 15. Configuración routing entre VLAN S2-----	48
Tabla 16. Configuración Router R1-----	51
Tabla 17. Verificación de conectividad de la red -----	52
Tabla 18. Configuración OSPF en R1 -----	53
Tabla 19. Configuración OSPF en R2 -----	54
Tabla 20. Configuración OSPFv3 en R2 -----	55
Tabla 21. Verificación OSPF_____	56
Tabla 22. Configuración de servidor de DHCP -----	57

LISTA DE TABLAS

Tabla 23. Configuración NAT estática y dinámica en R2-----	58
Tabla 24. Verificar el protocolo DHCP y la NAT estática -----	62
Tabla 25. Configurar NTP _____	63
Tabla 26. Restricción en líneas VTY en el R2-----	65
Tabla 27. Comando de CLI _____	66

LISTA DE FIGURAS

Figura 1. Escenario 1_____	11
Figura 2. R1 Desactivar las búsquedas DNS -----	14
Figura 3. R1 Nombre del router_____	14
Figura 4. R1 Nombre del dominio_____	14
Figura 5. R1 Contraseña modo EXEC -----	15
Figura 6. R1 Contraseña de acceso a la consola -----	15
Figura 7. R1 Longitud mínima para contraseñas -----	15
Figura 8. R1 Usuario administrador BD -----	16
Figura 9. R1 Sesión líneas VTY _____	16
Figura 10. R1 Configuración VTY _____	16
Figura 11. R1 Cifrar contraseñas de texto -----	16
Figura 12. R1 Configuración MOTD Banner -----	17
Figura 13. R1 Configuración interfaz g0/0/0 -----	17
Figura 14. R1 Configuración interfaz g0/0/1 -----	18
Figura 15. R1 Clave de cifrado RSA -----	18
Figura 16. S1 Desactivar búsqueda DNS -----	19
Figura 17. S1 Nombre del Switch -----	19
Figura 18. S1 Nombre del dominio -----	19
Figura 19. S1 Contraseña de acceso a consola -----	20
Figura 20. S1 Usuario administrador de BD -----	20
Figura 21. S1 Sesión de líneas VTY -----	20
Figura 22. S1 Configuración VTY -----	20
Figura 23. S1 Cifrar contraseñas de texto -----	21

LISTA DE FIGURAS

Figura 24. S1 Configuración MOTD Banner -----	21
Figura 25. S1 Clave cifrada RSA_____	21
Figura 26. S1 Configuración de interfaz administrador-----	22
Figura 27. PC_A Comando ipconfig/all-----	23
Figura 28. PC_B Comando ipconfig/all -----	24
Figura 26. Startup-config routers_____	29
Figura27. Reinicio de Router_____	30
Figura 28. Eliminación de archivos starup-config -----	31
Figura 29. Reinicio de router_____	32
Figura 30. Verificación en memoria flash -----	32
Figura 31. Configuración del Servidor -----	32
Figura 32. Comando ip domain-lookup -----	34
Figura 33. Asignación de nombre al Router -----	35
Figura 34. Asignación de contraseña -----	35
Figura 35. Contraseña de modo privilegiado -----	35
Figura 36. Contraseña Telnet_____	35
Figura 37. Encriptación de contraseñas -----	36
Figura 38. Mensaje de acceso no autorizado -----	36
Figura 39. Desactivar búsqueda DNS-----	38
Figura 40. Asignación de nombre a Router -----	38
Figura 41. Asignación de contraseña -----	38
Figura 42. Asignación de contraseña en consola -----	38

LISTA DE FIGURAS

Figura 43. Asignación de contraseña de acceso Telnet -----	38
Figura 44. Encriptación de contraseña -----	39
Figura 45. Habilitación de HTTP -----	39
Figura 46. Configuración de mensaje informativo -----	39
Figura 47. Configuración de Router R3 -----	41
Figura 48. Configuración del switch S1 -----	42
Figura 49. Ping 172.16 1.2 -----	44
Figura 50. Ping 172.16 2.1 -----	44
Figura 51. Creación de base de datos de VLAN -----	51
Figura 52. Dirección IP de administración -----	46
Figura 53. Asignación del gateway predeterminado -----	46
Figura 54. Enlace troncal en la interfaz F0/3 -----	46
Figura 55. Enlace troncal en la interfaz F0/5 -----	46
Figura 56. Configuración de puertos como puertos de acceso -----	46
Figura 57. Asignación de F0/6 a la VLAN 21 -----	46
Figura 58. Apagar todos los puertos sin usar -----	47
Figura 59. Base de datos de VLAN -----	48
Figura 60. Dirección IP de administración -----	49
Figura 61. Gateway predeterminado -----	49
Figura 62. Enlace troncal en la interfaz F0/3 -----	49
Figura 63. Configuración de puertos como puertos de acceso -----	49
Figura 64. Asignación F0/18 a la VLAN 21 -----	49
Figura 65. Apagar todos los puertos sin usar -----	50

LISTA DE FIGURAS

Figura 66. Configurar la subinterfaz 802.1Q .21 en G0/0/1 -----	51
Figura 67. Configuración de la subinterfaz 802.1Q .23 en G0/0/1 -----	51
Figura 68. Configuración la subinterfaz 802.1Q .99 en G0/0/1 -----	51
Figura 69. Activación de la interfaz G0/0/0-----	52
Figura 70. Ping 192.168 99.2_____	52
Figura 71. Ping 192.168 99.3_____	53
Figura 72. Configuración de OSPF área 0 -----	53
Figura 73. Redes conectadas directamente -----	54
Figura 74. Interfaces LAN como pasivas -----	54
Figura 75. Configurar OSPF área 0-----	54
Figura 76. Redes conectadas directamente-----	55
Figura 77. Interfaz LAN (loopback) como pasiva-----	55

GLOSARIO

Convergencia: estado estable que alcanza un conjunto de routers en un sistema autosuficiente de enrutamiento de tal forma que cada uno tiene pleno entendimiento de la mejor ruta hacia cada destino interno y externo y de las probables rutas alternativas en caso de fallas o cambios repentinos, comentado estado se consigue luego de un proceso de trueque de información cuyo algoritmo y tiempo de actitud frente a cambios repentinos en la red es dependiente del protocolo de enrutamiento en cuestión y su enfoque.

Cisco: es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro

Enrutamiento: labor indispensable para las comunicaciones remotas ejecutada por routers y switches multinivel que interconectan diferentes redes, por medio de tablas de enrutamiento y rutas predefinidas o automáticas con protocolos de enrutamiento deciden la mejor ruta para cada paquete basado en su información de red destino.

Gateway: es un dispositivo que posibilita interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación, su objetivo es traducir la información del protocolo usado en una red al protocolo utilizado en la red de destino.

CCNA: Las Certificaciones Cisco son internacionalmente reconocidas y se han convertido en un estándar para el área de las comunicaciones, las mismas aportan una gran credibilidad y alta reputación.

Redes: Es un conjunto de elementos con características comunes interconectadas o conectadas a través de un medio físico común, con el objetivo de compartir y optimizar recursos a través de una disposición física en particular.

Electrónica: La electrónica trata con circuitos eléctricos que involucran componentes eléctricos activos como tubos de vacío, transistores, diodos, circuitos integrados, optoelectrónica y sensores, asociados con componentes eléctricos pasivos y tecnologías de interconexión. Generalmente los dispositivos electrónicos contienen circuitos que consisten principalmente, o exclusivamente, en semiconductores activos complementados con elementos pasivos; tal circuito se describe como un circuito electrónico.

RESUMEN

En el desarrollo del siguiente trabajo se abarcan dos escenarios posibles, los cuales presentan diferentes requerimientos y necesidades en los puntos las redes de la plataforma Cisco, donde se detalla todo lo visto en el transcurso de cada periodo académico, donde se soporta de forma minuciosa con imágenes de las soluciones posibles en cada uno de los ítems.

En dichos escenarios se evidencia el uso de protocolos de enrutamiento OSPF y EIGRP, y la asignación de VLAN a las interfaces de redes específicas en todos los Switches, llevando a cabo la conmutación de la señal de las redes a partir de los principios hasta el destino solicitado, llevando a cabo implementaciones avanzadas de protocolos de enrutamiento, que en un escenario de la vida real será de gran utilidad para dar solución a posibles problemas y fallas de la red.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In the development of the following work, two possible scenarios are covered, which present different requirements and needs in the points of the Cisco platform networks, where everything seen in the course of each academic period is detailed, where it is thoroughly supported with images of the possible solutions in each of the articles.

In these scenarios, the use of OSPF and EIGRP routing protocols is evidenced, as well as the assignment of VLANs to the specific network interfaces in all the Switches, carrying out the switching of the signal of the networks from the principles to the destination. requesting, carrying out advanced implementations of routing protocols, which in a real life scenario will be very useful to solve possible problems and failures of the network.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

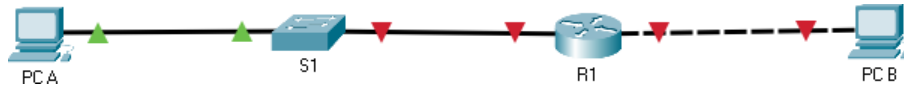
En el transcurso del diplomado CCNP de CISCO fue evidente la composición del mismo, en donde abarcamos temas de configuración como Routing & Switching, se busca adquirir y poner en practica conocimientos avanzados y a profundidad para la implementación efectiva de redes en múltiples escenarios incluyendo entornos corporativos de gran escala intentando solucionar posibles fallas haciendo uso de la versatilidad y escalabilidad de los dispositivos CISCO haciendo uso de las herramientas, técnicas, protocolos y servicios relacionados que son parte fundamental en el desarrollo de los escenarios.

Por otro lado, es indispensable tener en cuenta que para poner a prueba los conocimientos y comprobar su aplicabilidad en escenarios reales se implementaron y analizaron dos escenarios para Routing y Switching respectivamente con ayuda de los simuladores Packet Tracer y GNS3, los cuales presentaban ciertos requerimientos específicos y de gran alcance, buscando identificar las diferentes causas de problemas de conectividad, perdida de transferencia de paquetes, falta de comunicación con los demás dispositivos dentro de una VLAN, fallas que probablemente serán muy comunes en una vida profesional real.

Finalmente podemos evidenciar las aptitudes lógicas y la capacidad de solventar problemas en escenarios los cuales buscan capacitar de forma competitiva para la vida real al estudiante y al futuro administrador de redes de telecomunicaciones dentro y fuera de entidades **públicas** y privadas.

1. ESCENARIO 1

Figura 1: Escenario 1



Fuente: Elaborado por Diego Fabián Camargo

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Direccionamiento Item

Tabla de direccionamiento Item	Requerimiento
Dirección de Red	192.168.40.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente: Guía de actividades.

Parte 3: Configure aspectos básicos Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Tareas de configuración para R1

Tarea	Especificación
Desactivar las búsquedas DNS	
Nombre del Router	R1
Nombre del dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	

Configurar interfaz G 0/0/0	Establezca la dirección Establece la dirección IPv4 Activar la interfaz
Configurar interfaz G 0/0/1	Establezca la dirección Establece la dirección IPv4 Activar la interfaz
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Elaborado por Diego Fabian Camargo

- Desactivar las búsquedas DNS

R1(config)# no ip domain-lookup

Figura 2: Desactivar las búsquedas DNS.

```
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain
Router(config)#no ip domain-
Router(config)#no ip domain-lookup
Router(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Nombre del router

R1(config)# hostname R1

Figura 3. R1 Nombre del router

```
Router(config)#
Router(config)#hostname R1
R1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo.

- Nombre del dominio

R1(config)# ip domain name ccna-lab.com

Figura 4. R1 Nombre del dominio

```
R1(config)#
R1(config)#
R1(config)#ip domain name ccna-lab.com
R1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo.

- Contraseña cifrada para el modo EXEC privilegiado

```
R1(config)# enable password ciscoconpass
R1(config)# exit
```

Figura 5. R1 Contraseña modo EXEC

```
R1(config)#
R1(config)#enable password ciscoconpass
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente: Elaborado por Diego Fabian Camargo.

- Contraseña de acceso a la consola

```
R1(config)# line console 0
R1(config)# password ciscoenpass
R1(config)# login
R1(config)# exit
```

Figura 6. R1 Contraseña de acceso a la consola

```
R1#
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console 0
R1(config-line)#password ciscoenpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo.

- Establecer la longitud mínima para las contraseñas

```
R1(config)# security password min-length 10
```

Figura 7. R1 Longitud mínima para contraseñas

```

R1(config)#
R1(config)#security password min-length 10
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

```



>

- Crear un usuario administrativo en la base de datos local

```
R1(config)# username admin password admin1pass
```

Figura 8. R1 Usuario administrador BD

```

R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#username admin password admin1pass
R1(config)#

```



Fuente: Elaborado por Diego Fabian Camargo.

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

```
R1(config)# line vty 0 4
```

```
R1(config)# login local
```

Figura 9. R1 Sesión líneas VTY

```

R1(config)#
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#

```



Fuente: Elaborado por Diego Fabian Camargo.

- Configurar VTY solo aceptando SSH

```
R1(config)# transport input ssh
```

```
R1(config)# exit
```

Figura 10. R1 Configuración VTY

```

R1(config-line)#
R1(config-line)#
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#

```

Fuente: Elaborado por Diego Fabian Camargo.

- Cifrar las contraseñas de texto no cifrado

```
R1(config)# service password-encryption
```

Figura 11. R1 Cifrar contraseñas de texto

```

R1(config)#
R1(config)#service password-e
R1(config)#service password-encryption
R1(config)#

```

Fuente: Elaborado por Diego Fabian Camargo.

- Configure un MOTD Banner

```
R1(config)# banner motd "Acceso denegado. Por favor pongase en contacto con el Administrador."
```

Figura 12. R1 Configuración MOTD Banner

```

R1(config)#
R1(config)#banner motd "Acceso denegado. Por favor pongase en contacto con el
Administrador."
R1#
%SYS-5-CONFIG_I: Configured from console by console

```

Fuente: Elaborado por Diego Fabian Camargo.

- Configurar interfaz G 0/0/0

```

R1(config)# interface G 0/0/0
R1(config)# ip address 192.168.62.129 255.255.255.192
R1(config)# no shutdown
R1(config)# exit

```

Figura 13. R1 Configuración interfaz g0/0/0


```

R1(config)#
R1(config)#interface g0/0/0
R1(config-if)#ip address 192.168.40.129 255.255.255.192
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

```



Fuente: Elaborado por Diego Fabian Camargo.

- Configurar interfaz G 0/0/1

```

R1(config)# interface G 0/0/1
R1(config)# ip address 192.168.62.1 255.255.255.128
R1(config)# no shutdown
R1(config)# exit

```


Figura 14. R1 Configuración interfaz g0/0/1

```

R1(config-if)#exit
R1(config)#interface g0/0/1
R1(config-if)#ip address 192.168.40.1 255.255.255.128
R1(config-if)#no shutdown

R1(config-if)#

```



Fuente: Elaborado por Diego Fabian Camargo

- Generar una clave de cifrado RSA

```

R1(config)# ip domain-name ccna-lab.com
R1(config)# crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```

Figura 15. R1 Clave de cifrado RSA

```
R1(config-if)#exit
R1(config)#ip domain-name ccna-lab.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

Las tareas de configuración del S1 incluyen:

Tabla 3. Tareas de configuración para S1

Tarea	Especificación
Desactivar las búsquedas DNS	
Nombre del Swicht	S1
Nombre del dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente: Elaborado por Diego Fabian Camargo

- Desactivar las búsquedas DNS

S1(config)# No ip domain-lookup

Figura 16. S1 Desactivar búsqueda DNS

```
S1>enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Nombre del swicht

```
S1(config)# hostname S1
```

Figura 17. S1 Nombre del Switch

```
S1(config)#
S1(config)#hostname S1
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Nombre del dominio

```
S1(config)# ip domain name ccna-lab.com
```

Figura 18. S1 Nombre del dominio

```
S1(config)#
S1(config)#ip domain name ccna-lab.com
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Contraseña cifrada para el modo EXEC privilegiado

```
S1(config)# enable password ciscoconpass
```

```
S1(config)# exit
```

Figura 18. S1 Nombre del dominio

```
S1(config)#
S1(config)#enable password ciscoconpass
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```


Fuente: Elaborado por Diego Fabian Camargo

- Contraseña de acceso a la consola


```
S1(config)# line console 0
S1(config)# password ciscoenpass
S1(config)# login
S1(config)# exit
```

Figura 19. S1 Contraseña de acceso a consola

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password ciscoenpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```




Fuente: Elaborado por Diego Fabian Camargo

- Crear un usuario administrativo en la base de datos local

```
S1(config)# username admin password admin1pass
```

Figura 20. S1 Usuario administrador de BD

```
S1(config)#
S1(config)#username admin password admin1pass
S1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

```
S1(config)# line vty 0 4
S1(config)# login local
```

Figura 21. S1 Sesión de líneas VTY

```
S1(config)#
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#
```



Fuente: Elaborado por Diego Fabian Camargo

- Configurar VTY solo aceptando SSH

```
S1(config)# transport input ssh
S1(config)# exit
```

Figura 22. S1 Configuración VTY

```
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Cifrar las contraseñas de texto no cifrado

S1(config)# service password-encryption

Figura 23. S1 Cifrar contraseñas de texto

```
S1(config)#
S1(config)#service password-e
S1(config)#service password-encryption
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Configure un MOTD Banner

S1(config)# banner motd "El Acceso al Swicht es restringido. Únicamente personal autorizado"

Figura 24. S1 Configuración MOTD Banner

```
S1(config)#
S1(config)#banner motd "Acceso denegado. Por favor pongase en contacto con el
Administrador."
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Generar una clave de cifrado RSA

S1(config)# ip domain-name ccna-lab.com

S1(config)# crypto key generate rsa

The name for the keys will be: R1.ccna-lab.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Figura 25. S1 Clave cifrada RSA

```
S1(config)#
S1(config)#ip domain-name ccna-lab.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

- Configurar la interfaz de administración (SVI)

```
S1(config)# interface S1 SVI
S1(config)# ip address 192.168.62.1 255.255.255.192
S1(config)# no shutdown
S1(config)# exit
```

Figura 26. S1 Configuración de interfaz administrador

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.40.1 255.255.255.192
S1(config-if)#no shutdown

S1(config-if)#
```

Fuente: Elaborado por Diego Fabian Camargo

Paso 2: Configurar los equipos

Configure los equipos host PC_A y PC_B conforme a la tabla de direccionamiento, registre las configuraciones de red del hosts con el comando **ipconfig / all**

Tabla 4. Configuración de equipos PC_A

PC_A Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	0030.A357.C46B
Dirección IP	192.168.40.2
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.40.1

Fuente: Elaborado por Diego Fabian Camargo

Figura 27. PC_A Comando ipconfig/all

```

C:\>
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix... : 
    Physical Address. . . . . : 0030.A357.C46B
    Link-local IPv6 Address . . . . . : FE80::230:A3FF:FE57:C46B
    IPv6 Address. . . . . : ::
    IPv4 Address. . . . . : 192.168.40.2
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway. . . . . : ::
                           : 192.168.40.1
    DHCP Servers. . . . . : 0.0.0.0
    DHCPv6 IAID. . . . . : 
    DHCPv6 Client DUID. . . . . : 00-01-00-01-6E-A1-99-B6-00-30-A3-57-C4-6B
    DNS Servers. . . . . : ::
                           : 0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix... : 
    Physical Address. . . . . : 0030.F266.4D50
    Link-local IPv6 Address . . . . . : ::
    IPv6 Address. . . . . : ::
    IPv4 Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway. . . . . : ::
                           : 0.0.0.0
    DHCP Servers. . . . . : 0.0.0.0
    DHCPv6 IAID. . . . . : 
    DHCPv6 Client DUID. . . . . : 00-01-00-01-6E-A1-99-B6-00-30-A3-57-C4-6B
    DNS Servers. . . . . : ::
                           : 0.0.0.0

C:\>
  
```

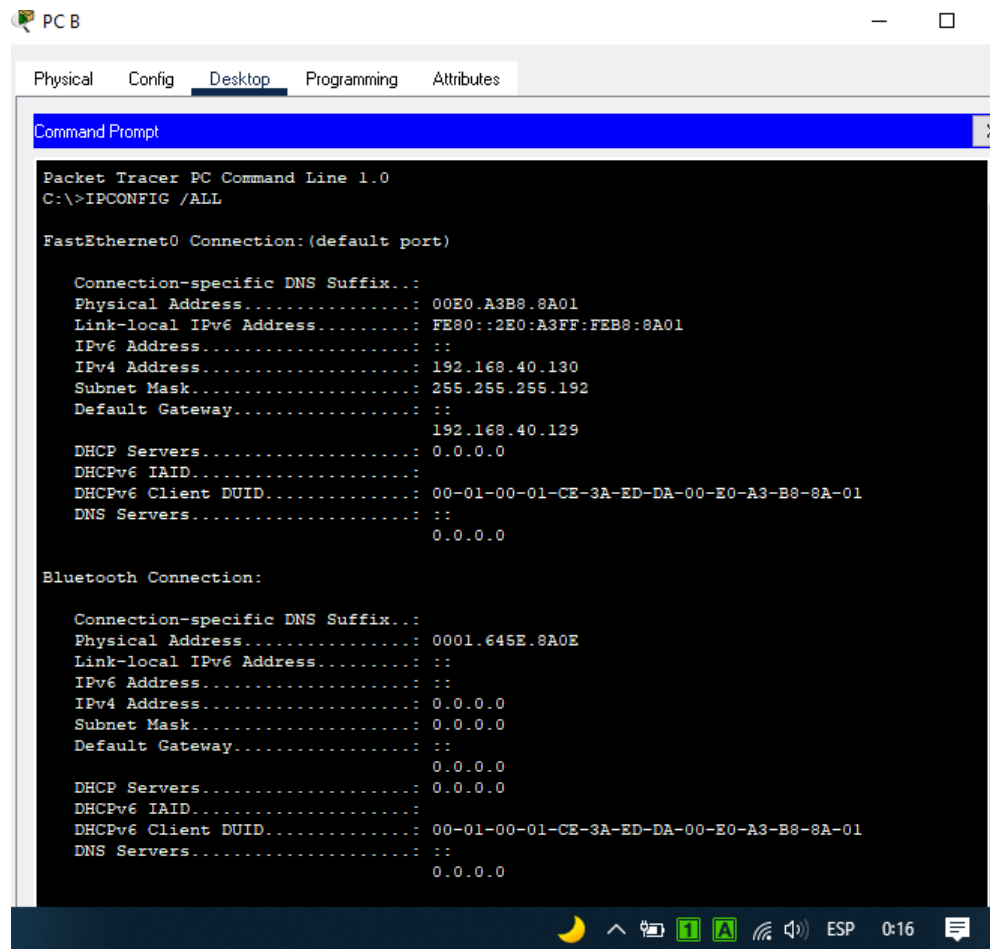
Fuente: Elaborado por Diego Fabian Camargo

Tabla 5. Configuración de equipos PC B

PC_B Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	00E0.A3B8.8A01
Dirección IP	192.168.40.130
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.40.129

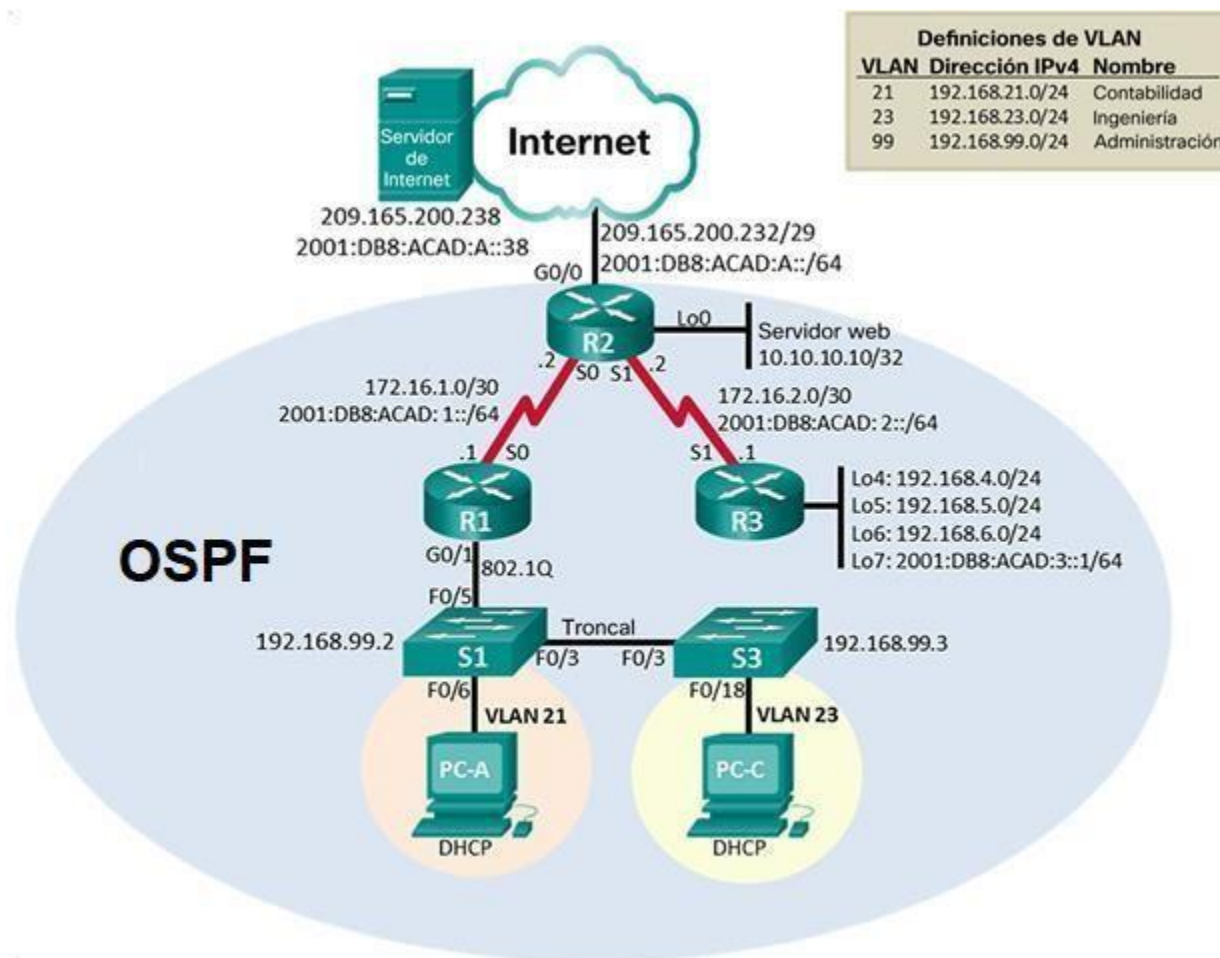
Fuente: Elaborado por Diego Fabian Camargo

Figura 28. PC_B Comando ipconfig/all



Fuente: Elaborado por Diego Fabian Camargo

Topología 2



Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6. Inicialización de Dispositivos

Tarea	Comando de IOS
-------	----------------

Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	SWITCH> enable SWITCH# erase startup-config SWITCH# delete flash:vlan.dat SWITCH# reload
Volver a cargar ambos switches	Switch# reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch# show flash

Fuente: Elaborado por Diego Fabian Camargo

Figura 26. Startup-config routers

```
Router>enable
Router#erase startp
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 27. Reinicio de Router

```
Router#
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####
```

Fuente: Elaborado por Diego Fabian Camargo

- Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

```
Switch> enable
Switch# erase startup-config
Switch# delete flash:vlan.dat
```

Figura 28. Eliminación de archivos starup-config

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

Ctrl+F6 to exit CLI focus

Copy

Fuente: Elaborado por Diego Fabian Camargo

- Volver a cargar ambos switches

```
Switch# reload
```

Figura 29. Reinicio de router

```
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)EX RELEASE SOFTWARE (fc4)
```

Ctrl+F6 to exit CLI focus

Copy

Fuente: Elaborado por Diego Fabian Camargo

- Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

```
Switch>enable
Switch# show flash
```


Figura 30. Verificación en memoria flash

```
Switch>enable
Switch#show flash
Directory of flash:/

 1  -rw-     4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
```

Fuente: Elaborado por Diego Fabian Camargo

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

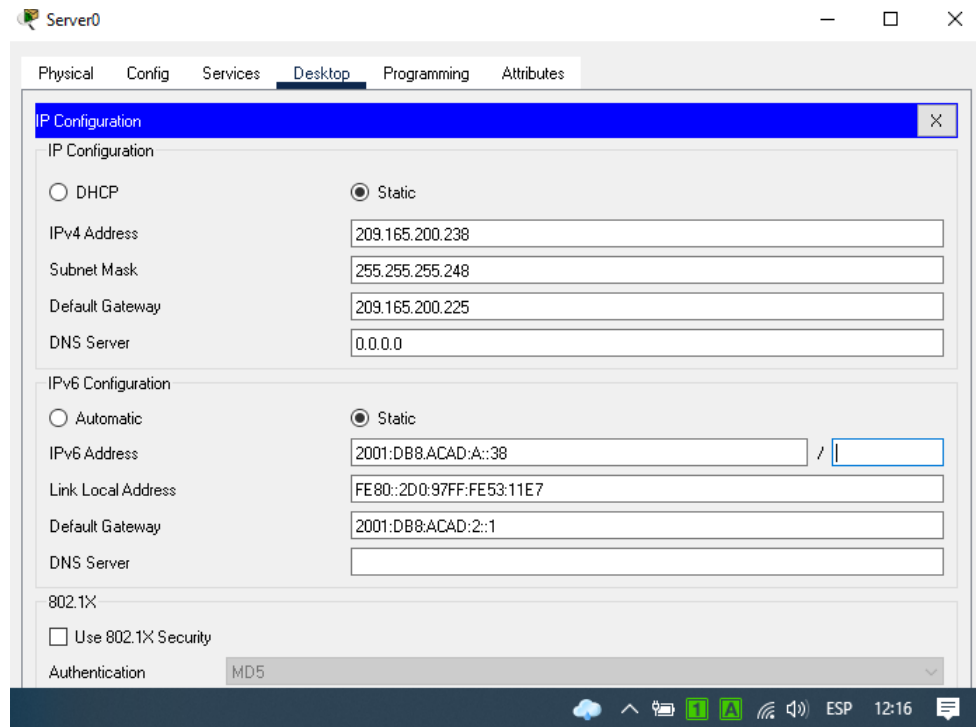
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 7. Configuración servidor internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Elaborado por Diego Fabian Camargo

Figura 31. Configuración del Servidor



Fuente: Elaborado por Diego Fabian Camargo

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración Router R1

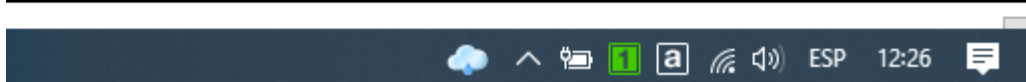
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login

Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "se prohíbe el acceso no autorizado"
Interfaz S0/1/0	R1(config)#int s0/1/0 R1(config-if)#description connection hacia R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#int s0/1/1 R1(config-if)#description connection hacia R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown

Fuente: Elaborado por Diego Fabian Camargo

Figura 32. Comando ip domain-lookup


```
Router>
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 33. Asignación de nombre al Router

```
Router(config)#
Router(config)#hostname R1
R1(config)#
```










Fuente: Elaborado por Diego Fabian Camargo

Figura 34. Asignación de contraseña

```
R1(config)#  
R1(config)#enable secret class  
R1(config)#
```

Ctrl+F6 to exit CLI focus

       ESP 12:32

Fuente: Elaborado por Diego Fabian Camargo

Figura 35. Contraseña de modo privilegiado

```
R1(config)#  
R1(config)#line console 0  
R1(config-line)#password cisco  
R1(config-line)#login  
R1(config-line)#
```

Ctrl+F6 to exit CLI focus

       ESP 12:35

Fuente: Elaborado por Diego Fabian Camargo

Figura 36. Contraseña Telnet

```
R1(config-line)#  
R1(config-line)#line vty 0 4  
R1(config-line)#password cisco  
R1(config-line)#login  
R1(config-line)#
```

Ctrl+F6 to exit CLI focus

       ESP 12:39

Fuente: Elaborado por Diego Fabian Camargo

Figura 37. Encriptación de contraseñas

```
R1(config-line)#service password-encryption  
R1(config)#
```

Ctrl+F6 to exit CLI focus

       ESP 12:42

Fuente: Elaborado por Diego Fabian Camargo

Figura 38. Mensaje de acceso no autorizado

```
R1(config)#
R1(config)#banner motd "se prohíbe el acceso no autorizado"
R1(config)#
R1(config)#
```

Ctrl+F6 to exit CLI focus



Fuente: Elaborado por Diego Fabian Camargo

Paso 3: Configurar R2

Tabla 9. Configuración Router R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server (Entrada invalida, este comando no funciona en Packet Tracer)
Mensaje MOTD	R2(config)#banner motd "Se prohíbe el acceso no autorizado"
Interfaz S0/1/0	R2(config)#int s0/1/0 R2(config-if)#description conectado a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64

	R2(config-if)#no shutdown
Interfaz S0/1/1	R2(config)#int s0/1/1 R2(config-if)#description conectado a R3 48 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config)#Clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description conectado a internet R2(config-if)#ip address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.252 R2(config-if)#description conectado a servidor web simulado R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Fuente: Elaborado por Diego Fabian Camargo

Figura 39. Desactivar búsqueda DNS

```
Router>enable
Router#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```

Ctrl+F6 to exit CLI focus

Copy Pas

ESP 18:55

Fuente: Elaborado por Diego Fabian Camargo

Figura 40. Asignación de nombre a Router

```
Router(config)#
Router(config)#hostname R2
R2(config)#
```

ESP 19:02

Fuente: Elaborado por Diego Fabian Camargo

Figura 41. Asignación de contraseña

```
R2(config)#
R2(config)#enable secret class
R2(config)#
```

ESP 19:04

Fuente: Elaborado por Diego Fabian Camargo

Figura 42. Asignación de contraseña en consola

```
R2(config)#
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

ESP 19:05

Fuente: Elaborado por Diego Fabian Camargo

Figura 43. Asignación de contraseña de acceso Telnet

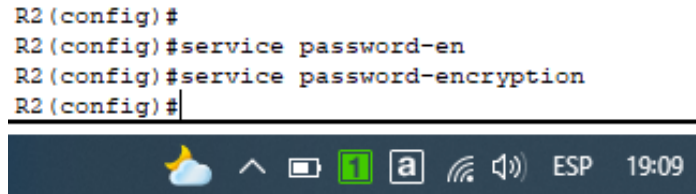
```
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

ESP 19:08

Fuente: Elaborado por Diego Fabian Camargo

Figura 44. Encriptación de contraseña

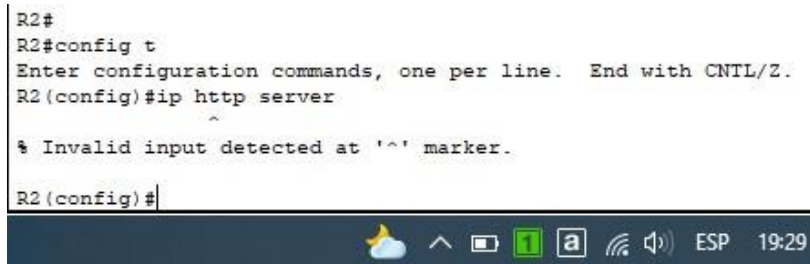
```
R2(config)#  
R2(config)#service password-en  
R2(config)#service password-encryption  
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 45. Habilitación de HTTP

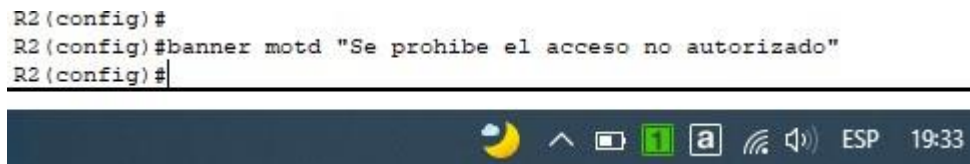
```
R2#  
R2#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)#ip http server  
^  
% Invalid input detected at '^' marker.  
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 46. Configuración de mensaje informativo

```
R2(config)#  
R2(config)#banner motd "Se prohíbe el acceso no autorizado"  
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

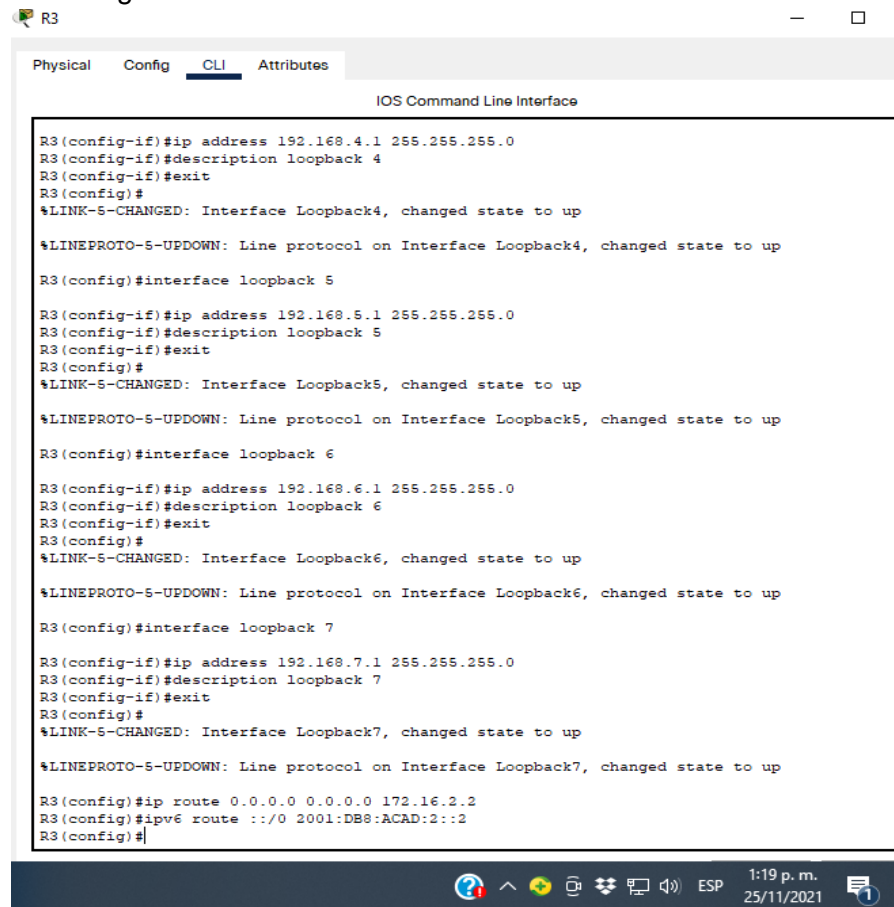
Tabla 10. Configuración Router R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohíbe el acceso no autorizado"
Interfaz S0/1/1	R3(config)#interface serial0/1/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#description conexion R2 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#description loopback 4 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#description loopback 5 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#description loopback 6 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ip address 192.168.7.1 255.255.255.0

	R3(config-if)#description loopback 7 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)# ipv6 route ::/0 2001:DB8:ACAD:2::2

Fuente: Elaborado por Diego Fabian Camargo

Figura 47. Configuración de Router R3



```

R3
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#description loopback 4
R3(config-if)#exit
R3(config)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R3(config)#interface loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#description loopback 5
R3(config-if)#exit
R3(config)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
R3(config)#interface loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#description loopback 6
R3(config-if)#exit
R3(config)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config)#interface loopback 7
R3(config-if)#ip address 192.168.7.1 255.255.255.0
R3(config-if)#description loopback 7
R3(config-if)#exit
R3(config)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2
R3(config)#

```

Fuente: Elaborado por Diego Fabian Camargo

Paso 5: Configurar S1

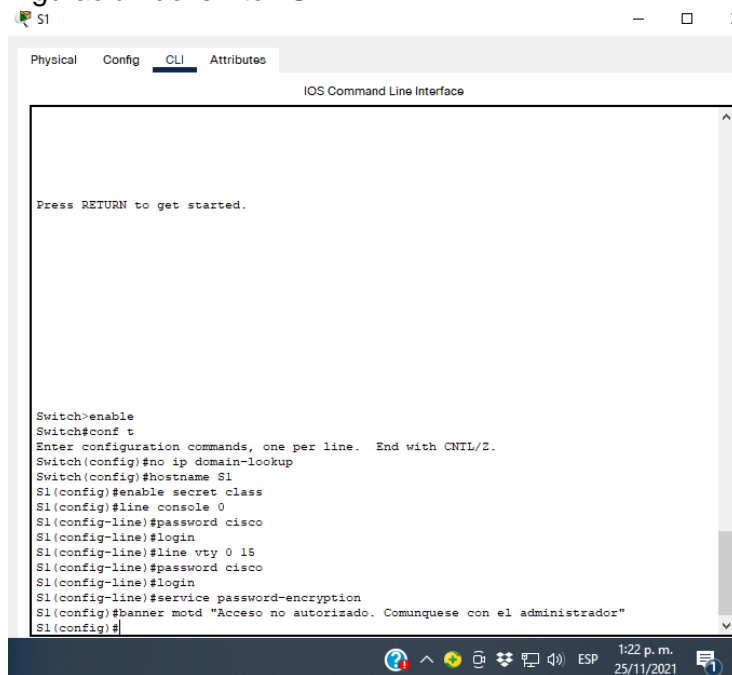
La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración Switch S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Se prohíbe el acceso no autorizado".

Fuente: Elaborado por Diego Fabian Camargo

Figura 48. Configuración del switch S1



```
S1
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTRL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd "Acceso no autorizado. Comunquese con el administrador"
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

Paso 6: Configurar el S2

La configuración del S2 incluye las siguientes tareas:

Tabla 12. Configuración Switch S2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login
Contraseña de acceso Telnet	S2(config-line)#line vty 0 15 S2(config-line)#password cisco S2(config-line)#login
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Mensaje MOTD	S2(config)#banner motd "Se prohíbe el acceso no autorizado".

Fuente: Elaborado por Diego Fabian Camargo

Paso 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Verificación de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	200.165.200.233	Null

Fuente: Elaborado por Diego Fabian Camargo


Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 49. Ping 172.16.1.2

```
R1>enable
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1#
```




Fuente: Elaborado por Diego Fabian Camargo

Figura 50. Ping 172.16.2.1

```
R1>enable
Password:
R1#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1#
```



Fuente: Elaborado por Diego Fabian Camargo

Parte 3: Configurar la seguridad del switch, las

VLAN y el routing entre VLAN Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración routing entre VLAN

Elemento o tarea de configuración	
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion
Asignar la dirección IP de administración.	interface vlan 99 ip address 192.168.99.2 255.255.255.0 exit
Asignar el gateway predeterminado	ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	interface f0/3 switchport mode trunk switchport trunk allowed vlan all switchport trunk native vlan 1 exit
Forzar el enlace troncal en la interfaz F0/5	interface f0/5 switchport mode trunk switchport trunk allowed vlan all switchport trunk native vlan 1 exit
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4, f0/6-24 switchport mode access no shutdown
Asignar F0/6 a la VLAN 21	int f0/6 switchport access vlan 21
Apagar todos los puertos sin usar	int range f0/1-2, f0/4, f0/7-24 shutdown

Fuente: Elaborado por Diego Fabian Camargo

Figura 51. Creación de base de datos de VLAN

```
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 52. Dirección IP de administración

```
S1(config-vlan)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
S1(config)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 53. Asignación del gateway predeterminado

```
S1(config)#ip default-gateway 192.168.99.1
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 54. Enlace troncal en la interfaz F0/3

```
S1(config-if)#switchport trunk allowed vlan all
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 55. Enlace troncal en la interfaz F0/5

```
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan all
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 56. Configuración de puertos como puertos de acceso

```
S1(config)#  
S1(config)#int range f0/1-2, f0/4, f0/6-24  
S1(config-if-range)#switchport mode access  
S1(config-if-range)#no shutdown  
S1(config-if-range)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 57. Asignación de F0/6 a la VLAN 21

```
S1(config-if-range)#  
S1(config-if-range)#int f0/6  
S1(config-if)#switchport access vlan 21  
S1(config-if)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 58. Apagar todos los puertos sin usar

```
S1(config-if)#int range f0/1-2, f0/4, f0/7-24  
S1(config-if-range)#shutdown  
  
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down  
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
```



Fuente: Elaborado por Diego Fabian Camargo

Paso 2: Configurar el S2

Tabla 15. Configuración routing entre VLAN S2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name administracion
Asignar la dirección IP de administración	interface vlan99 ip address 192.168.99.3 255.255.255.0 exit
Asignar el gateway predeterminado.	ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	int f0/3 switchport mode trunk switchport trunk allowed vlan all switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4-24 switchport mode access
Asignar F0/18 a la VLAN 21	int f0/18 switchport access vlan 23
Apagar todos los puertos sin usar	int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

Fuente: Elaborado por Diego Fabian Camargo

Figura 59. Base de datos de VLAN

```
S2>enable
Password:
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 21
S2(config-vlan)#name Contabilidad
S2(config-vlan)#vlan 23
S2(config-vlan)#name Ingenieria
S2(config-vlan)#vlan 99
S2(config-vlan)#name administracion
S2(config-vlan)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 60. Dirección IP de administración

```
S2(config-vlan)#interface vlan99
S2(config-if)#ip address 192.168.99.3 255.255.255.0
S2(config-if)#exit
S2(config)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S2(config)#
```

3:55 p. m.
25/11/2021

Fuente: Elaborado por Diego Fabian Camargo

Figura 61. Gateway predeterminado

```
S2(config)#ip default-gateway 192.168.99.1
S2(config)#
```

3:57 p. m.
25/11/2021

Fuente: Elaborado por Diego Fabian Camargo

Figura 62. Enlace troncal en la interfaz F0/3

```
S2(config)#
S2(config)#int f0/3
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan all
S2(config-if)#switchport trunk native vlan 1
S2(config-if)#
```

3:57 p. m.
25/11/2021

Fuente: Elaborado por Diego Fabian Camargo

Figura 63. Configuración de puertos como puertos de acceso

```
S2(config-if)#
S2(config-if)#int range f0/1-2, f0/4-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%SPANTRIE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/2 VLAN1.

%SPANTRIE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/2 on VLAN0001. Inconsistent port
type.
```

3:58 p. m.
25/11/2021

Fuente: Elaborado por Diego Fabian Camargo

Figura 64. Asignación F0/18 a la VLAN 21

```
S2(config-if-range)#int f0/18
S2(config-if)#switchport access vlan 23
S2(config-if)#
```

3:58 p. m.
25/11/2021

Fuente: Elaborado por Diego Fabian Camargo

Figura 65. Apagar todos los puertos sin usar

```
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S2 (config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

Fuente: Elaborado por Diego Fabian Camargo

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración Router R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 enG0/1	interface g0/0/1.21 encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0 description vlan 21 no shutdown exit
Configurar la subinterfaz 802.1Q .23 enG0/0/0	interface gigabitEthernet0/0/1.23 encapsulation dot1Q 23 ip address 192.168.23.1 255.255.255.0 description vlan 23 no shutdown exit
Configurar la subinterfaz 802.1Q .99 enG0/0/0	interface g0/0/1.99 encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0 description vlan 99 shutdown exit

Activar la interfaz G0/0/0	interface g0/0/0 no shutdown
----------------------------	---------------------------------

Fuente: Elaborado por Diego Fabian Camargo

Figura 66. Configurar la subinterfaz 802.1Q .21 en G0/0/1

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0/1.21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#description vlan 21
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 67. Configuración de la subinterfaz 802.1Q .23 en G0/0/1

```
R1(config)#
R1(config)#interface gigabitEthernet0/0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#description vlan 23
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 68. Configuración la subinterfaz 802.1Q .99 en G0/0/1

```
R1(config)#
R1(config)#interface g0/0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#description vlan 99
R1(config-subif)#shutdown
R1(config-subif)#exit
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 69. Activación de la interfaz G0/0/0

```
R1(config)#interface g0/0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.23, changed state to up
|
```



Fuente: Elaborado por Diego Fabian Camargo

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Verificación de conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	Exitoso
S2	R1, dirección VLAN 99	192.168.99.3	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Null
S2	R1, dirección VLAN 23	192.168.23.1	Null

Fuente: Elaborado por Diego Fabian Camargo

Figura 70. Ping 192.168.99.2

```
S1#
S1#ping 192.168.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/8 ms

S1#|
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 71. Ping 192.168.99.3

```
S2>enable
Password:
S2#ping 192.168.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/11 ms

S2#
```

Fuente: Elaborado por Diego Fabian Camargo

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 router-id 1.1.1.1
Anunciar las redes conectadas directamente	network 172.16.1.0 0.0.0.3 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	passive-interface g0/0/1.21 passive-interface g0/0/1.23 passive-interface g0/0/1.99
Desactive la sumarización automática	no

Fuente: Elaborado por Diego Fabian Camargo

Figura 72. Configuración de OSPF área 0

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#
R1(config-router)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 73. Redes conectadas directamente

```

R1(config-router)#
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#

```



Fuente: Elaborado por Diego Fabian Camargo

Figura 74. Interfaces LAN como pasivas

```

R1(config-router)#passive-interface g0/0/1.21
R1(config-router)#passive-interface g0/0/1.23
R1(config-router)#passive-interface g0/0/1.99
R1(config-router)#

```



Fuente: Elaborado por Diego Fabian Camargo

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configuración OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 router-id 2.2.2.2
Anunciar las redes conectadas directamente	network 10.10.10.10 0.0.0.0 area 0 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area
Establecer la interfaz LAN (loopback) como pasiva	passive-interface lo0
Desactive la sumalización automática.	no

Fuente: Elaborado por Diego Fabian Camargo

Figura 75. Configurar OSPF área 0

```

R1(config)#router ospf 1
R1(config-router)#router-id 2.2.2.2
R1(config-router)#

```



Fuente: Elaborado por Diego Fabian Camargo

Figura 76. Redes conectadas directamente

```
R1(config-router)#
R1(config-router)#network 10.10.10.10 0.0.0.0 area 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 172.16.2.0 0.0.0.3 area 0
R1(config-router)#
00:23:01: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/1/0 from LOADING to FULL,
Loading Done
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 77. Interfaz LAN (loopback) como pasiva

```
R1(config-router)#passive-interface lo0
R1(config-router)#
```

Fuente: Elaborado por Diego Fabian Camargo

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración OSPFv3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	network 192.168.4.0 0.0.0.255 area 0 network 192.168.5.0 0.0.0.255 area 0 network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface lo4 passive-interface lo5 passive-interface lo6
Desactive la sumarización automática.	no

Fuente: Elaborado por Diego Fabian Camargo

Figura 78. Configuración de OSPF área 0

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 79. Redes IPv4 conectadas directamente

```
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 80. Interfaces de LAN IPv4 (Loopback) como pasivas

```
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#
```



Fuente: Elaborado por Diego Fabian Camargo

Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21. Verificación OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocol
¿Qué comando muestra solo las rutas OSPF?	
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf

Fuente: Elaborado por Diego Fabian Camargo

Figura 81. Show ip protocol

```
R1#Show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:04:20
    2.2.2.2          110          00:04:20
  Distance: (default is 110)

R1#
```

Fuente: Elaborado por Diego Fabian Camargo

Figura 82. Show ip ospf

```
R1#Show ip ospf

Routing Process "ospf 1" with ID 2.2.2.2
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of external LSA 0, Checksum Sum 0x000000
  Number of opaque AS LSA 0, Checksum Sum 0x000000
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  External flood list length 0
    Area BACKBONE(0)
      Number of interfaces in this area is 3
      Area has no authentication
      SPF algorithm executed 1 times
      Area ranges are
        Number of LSA 2, Checksum Sum 0x00f833
        Number of opaque link LSA 0, Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Fuente: Elaborado por Diego Fabian Camargo

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

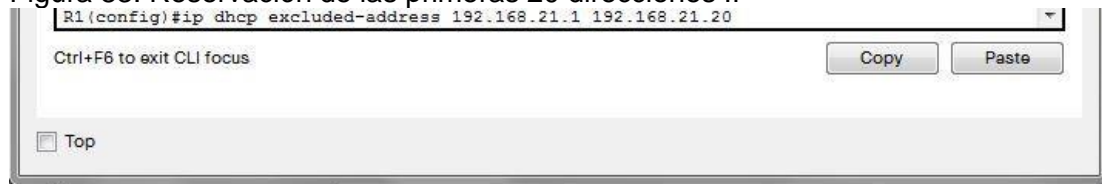
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración de servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.21 dns-server 10.10.10.10 domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.21 dns-server 10.10.10.10 domain-name ccna-sa.com

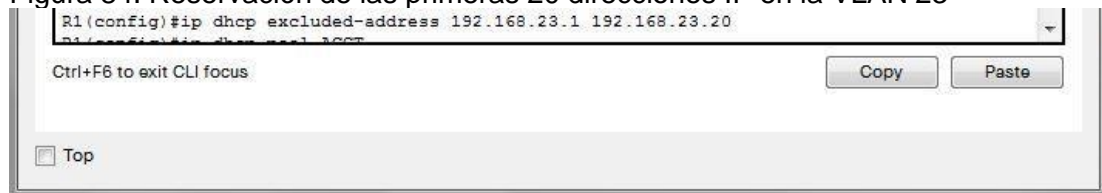
Fuente: Elaborado por Diego Fabian Camargo

Figura 83. Reservación de las primeras 20 direcciones IP



Fuente: Elaborado por Diego Fabian Camargo

Figura 84. Reservación de las primeras 20 direcciones IP en la VLAN 23



Fuente: Elaborado por Diego Fabian Camargo

Figura 85. Pool de DHCP para la VLAN 21

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente: Elaborado por Diego Fabian Camargo

Figura 86. Creación un pool de DHCP para la VLAN 23

```
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#exit
R1(config)#exit
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente: Elaborado por Diego Fabian Camargo

Paso 2: Configurar la NAT
estática y dinámica en el R2

Tabla 23. Configuración NAT estática y dinámica en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con unacuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 username webuser privilege 15 secret 5 cisco12345
Habilitar el servicio del servidor HTTP	ip http server
Configurar el servidor HTTP para utilizar labase de datos local para la autenticación	ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229

	ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	int g0/0/1 ip nat outside int s0/1/0 ip nat inside int s0/1/1 ip nat inside exit
Configurar la NAT dinámica dentro de una ACL privada	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255 access-list 1 permit 192.168.5.0 0.0.3.255 access-list 1 permit 192.168.6.0 0.0.3.255 access-list 1 permit 2001:DB8:ACAD:3::1 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.28
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Fuente: Elaborado por Diego Fabian Camargo

Figura 87. Base de datos local con cuenta de usuario

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#username admin privilege 15 secret 5 system
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 88. Habilitar el servicio del servidor HTTP

```
R1(config)#
R1(config)#ip http server
^
% Invalid input detected at '^' marker.
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 89. Configuración del servidor HTTP para base de datos local

```

R1(config)#ip http authentication local
^
% Invalid input detected at '^' marker.

R1(config)#

```

Fuente: Elaborado por Diego Fabian Camargo

Figura 90. NAT estática al servidor web

```

R1(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R1(config)#

```

Fuente: Elaborado por Diego Fabian Camargo

Figura 91. Interfaz interna y externa para la NAT estática

```

R1(config)#int g0/0/1
R1(config-if)#ip nat outside
R1(config-if)#int s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#int s0/1/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#

```

Fuente: Elaborado por Diego Fabian Camargo

Figura 92. NAT dinámica dentro de una ACL privada

```

R1(config)#
R1(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.4.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.5.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.6.0 0.0.0.255
R1(config)#access-list 1 permit 2001:DB8:ACAD:3::1 0.0.0.3.255
^
% Invalid input detected at '^' marker.

R1(config)#

```

Fuente: Elaborado por Diego Fabian Camargo

Figura 93. Pool de direcciones IP públicas utilizables

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#username webuser privilege 15 secret 5 cisco12345
R1(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.28
%Pool INTERNET mask 255.255.255.28 too small; should be at least 255.255.255.252
%Start and end addresses on different subnets
R1(config)#ip nat inside source list 1 pool INTERNET
R1(config)#
```

Fuente: Elaborado por Diego Fabian Camargo

Paso 3: Verificar el protocolo DHCP y la NAT estática

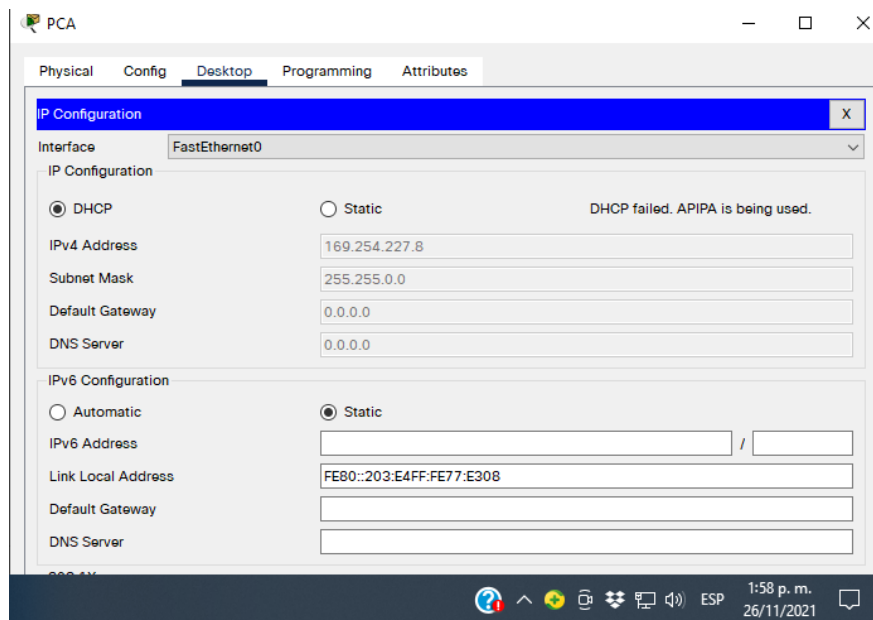
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pingse realicen correctamente.

Tabla 24. Verificar el protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ip Address 169.254.227.8 Subnet Mask 255.255.255.0
Verificar que la PC-B haya adquirido información de IP del servidor de DHCP	Ip Address 169.254.229.6 Subnet Mask 255.255.255.0
Verificar que la PC-A pueda hacer ping ala PC-B Nota: Quizá sea necesario deshabilitar elfirewall de la PC.	null
Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	null

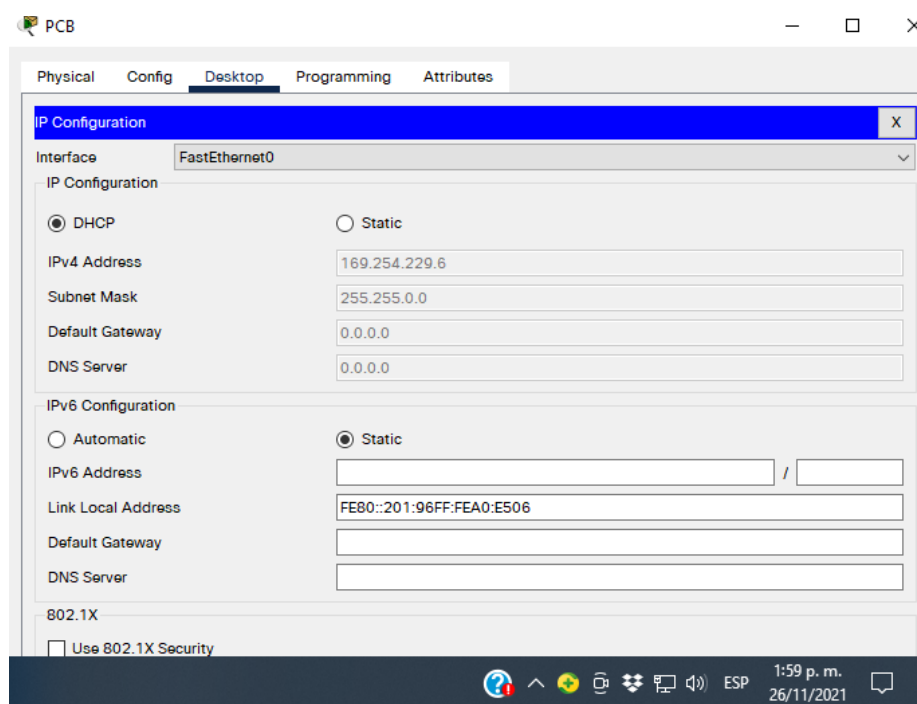
Fuente: Elaborado por Diego Fabian Camargo

Figura 94. Verificación dirección DHCP



Fuente: Elaborado por Diego Fabian Camargo

Figura 95. Verificación de direccionamiento DHCP PCB



Fuente: Elaborado por Diego Fabian Camargo

Parte 6: Configurar NTP

Tabla 25. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	ntp master 5
Configurar R1 como un cliente NTP.	ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar
Verifique la configuración de NTP en R1.	show ntp associations

Fuente: Elaborado por Diego Fabian Camargo

Figura 96. Ajuste de fecha y hora R2



Fuente: Elaborado por Diego Fabian Camargo

Figura 97. Configuración R2 como un maestro NTP

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 98. Configuración R1 como un cliente NTP.

```
R1(config)#ntp server 172.16.1.2
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 99. Configuración R1 para actualizaciones de calendario periódicas

```
R1(config)#ntp update-calendar
R1(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 100. Verificación de la configuración de NTP en R1.

```
R1#show ntp associations

address      ref clock      st  when  poll  reach  delay  offset
disp
~172.16.1.2  127.127.1.1    5   12    16    17     5.00   -558912.00
0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```



Fuente: Elaborado por Diego Fabian Camargo

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Restricción en líneas VTY en el R2


Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1	ip access-list standard ADMIN-MGT permit host 172.16.1.2

establezca una conexión Telnet con R2	exit
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in exit
Permitir acceso por Telnet a las líneas de VTY	line vty 0 4 transport input telnet exit
Verificar que la ACL funcione como se espera	telnet Host: 172.16.1.2

Fuente: Elaborado por Diego Fabian Camargo

Figura 101. Lista de acceso R2


```
R2>enable
Password:
R2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.2
R2(config-std-nacl)#exit
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 102. ACL con nombre a las líneas VTY R2


```
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 103. Telnet a las líneas de VTY

```
R2(config)#line vty 0 4
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 104. Verificación que la ACL

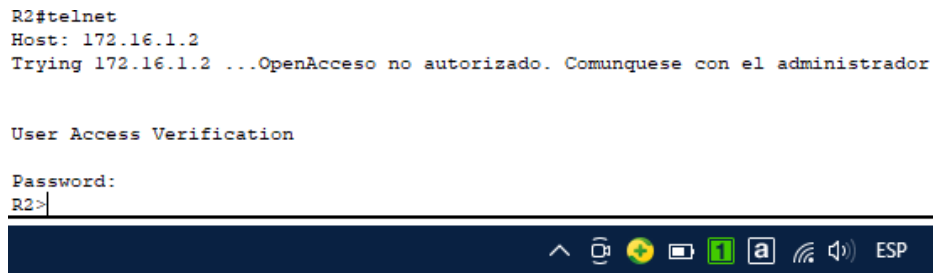
```

R2#telnet
Host: 172.16.1.2
Trying 172.16.1.2 ...OpenAcceso no autorizado. Comunquese con el administrador

User Access Verification

Password:
R2>

```



Fuente: Elaborado por Diego Fabian Camargo

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 27. Comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show ip access-list
Restablecer los contadores de una lista de acceso	Clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección que se aplica?	Show ip interface s0/1/1
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation *

Fuente: Elaborado por Diego Fabian Camargo

Figura 105. Lista de acceso desde la última vez

```
R2#Show ip access-list
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.2 (2 match(es))
```

R2#



Fuente: Elaborado por Diego Fabian Camargo

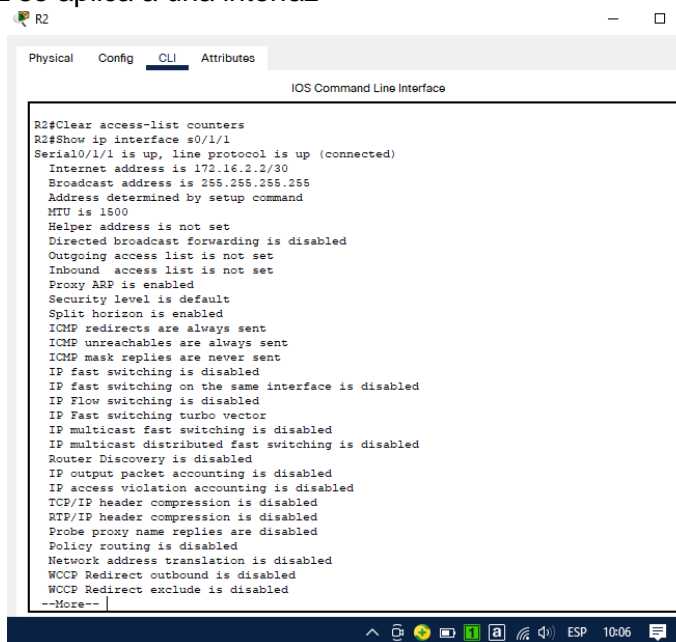
Figura 106. Restablecimiento de los contadores

```
R2#Clear access-list counters
R2#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 107. ACL se aplica a una interfaz



Fuente: Elaborado por Diego Fabian Camargo

Figura 108. Traducciones NAT

```
R2#Show ip nat translations  
R2#
```



Fuente: Elaborado por Diego Fabian Camargo

Figura 109. Eliminación de traducciones de NAT dinámicas

```
R2#Clear ip nat translation *  
R2#
```



Fuente: Elaborado por Diego Fabian Camargo

CONCLUSIONES

Los protocolos de enrutamiento dinámico OSPF y EIGRP funcionan con lógicas y métricas diferentes sin embargo permiten integrarse de forma sencilla y funcionar de forma flexible y eficiente por medio de la técnica de redistribución de rutas en escenarios que requieran la coexistencia en medio de éstos y otros protocolos, se observa una más grande versatilidad de configuración en EIGRP.

Las técnicas de adición de enlaces y control de redundancia de capa 2 son subjetivamente complicados de llevar a cabo ya que se tienen que mantener el control de distintas cambiantes entre los diversos puertos y grupos que participan en asociaciones de diversos enlaces redundantes, se debería tener particular cuidado en garantizar la compatibilidad de fronteras entre switches capa 2 y switches multinivel, generalmente es necesario asegurar una completa coherencia de fronteras de switchport no solo para el establecimiento de agrupaciones en interfaces físicas en EtherChannel L2 y L3, sino para que también resulte óptimo y lógico el control de loop por medio de la configuración de puentes raíz de Spanning-tree, empero esto no es más grande problema si se cuenta con un conveniente entrenamiento en técnicas de troubleshooting que identifiquen un potencial problema y puedan obtener como consecuencia redes con bastante buenas prestaciones.

Al configurar una VLAN en un switch es fundamental considerar que éstas comparten el ancho de banda, por esto se necesitan medidas de estabilidad extras como la asignación de un número de VLAN nativo exclusivo a los puertos de enlace troncal, definir las VLAN a mover sobre los enlaces troncales, desactivar el protocolo de enlace troncal VTP, de lo opuesto tienen que configurarse su dominio de administración.

BIBLIOGRAFÍA

AREAIP. (s.f.). Comandos Ethernetchannel o Portchannel con LACP y PAGP. Recuperado de http://areaip.blogspot.com/2016/09/comandos-ethernetchannel-o-portchannel_24.html

CISCO. (s.f.) Cómo comprender VLAN Trunk Protocol (VTP) . Recuperado de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.pdf

CISCO. (2020). Configure InverVLAN Routing on Layer 3 Switches. Recuperado de <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYeiNT1lInWR0hoMxgBNv1CJ>

Sagar, Azeem, A. (2020) CCNP ENTERPRISE 2020. ENCOR 350-401 ENARSI 300-410 For enrolling in Online “CCNP Enterprise” batch. Recuperado de <http://www.networkjourney.com/wp-content/uploads/2020/04/ccnpenterpriseworkbookv1-200418043231.pdf>